Nota Técnica

Tecnologias e riscos: armas cibernéticas

Samuel César da Cruz Júnior

Nº 11

Brasília, julho de 2013

ipea Por um Brasil desenvolvido

ipea Instituto de Pesquisa Econômica Aplicada

Nota Técnica

TECNOLOGIAS E RISCOS: ARMAS CIBERNÉTICAS*

Samuel César Da Cruz Júnior[1]

1. INTRODUÇÃO

A sociedade contemporânea tem se tornado dependente de processos autônomos. Nos últimos anos, houve um desenvolvimento intenso da eletrônica, computação e sistemas mecânicos de precisão, que difundiram amplamente os dispositivos computacionais bem como a interligação deles em rede. Como resultado, aumentaram também as vulnerabilidades de sistemas críticos, colocando em risco até mesmo a soberania nacional. No caso brasileiro, nas mais de 320 redes do Governo Federal são identificados em torno de três mil incidentes virtuais de segurança por mês (GSI/PR, 2013). Este texto tem por objetivo apresentar os riscos e ameaças inerentes às tecnologias da informação e comunicação e ainda busca mostrar como essas ameaças podem ser mitigadas ao se conhecer os mecanismos normalmente utilizados em ataques cibernéticos.

Os sistemas computacionais e a internet têm alterado rapidamente os parâmetros do cotidiano humano (AMORIM, 2012). O rápido crescimento da computação ubíqua[2] tem mudado hábitos e o dia-a-dia das pessoas, tornando-as mais ágeis, informadas, interconectadas e produtivas. Basta lembrar que, há pouco mais de cinquenta anos, para se conseguir estabelecer uma comunicação entre dois pontos era preciso falar com uma telefonista para que ela fizesse a conexão física entre os interlocutores. Hoje, sistemas autônomos são capazes de fazer milhões de comutações de chamadas em segundos.

Sistemas bancários, transporte urbano, aviação, saneamento, sistemas de saúde, guarda civil, telecomunicações e sistemas elétricos são apenas alguns exemplos de infraestruturas críticas fortemente dependentes dos sistemas computacionais. Tais sistemas precisam funcionar online e estar permanentemente disponíveis. Por consequência, a confiabilidade e segurança deles são elementos cruciais.

Eventuais falhas ou indisponibilidade em qualquer das infraestruturas críticas são suficientes para causar, além de prejuízos financeiros, perdas sociais diversas. Assim, na medida em que o bem-estar e a segurança da sociedade passam a depender da segurança cibernética, ela se torna um dever do Estado e não apenas mais um item de maior ou menor prioridade de um governo.

Sistemas de proteção cibernética robustos dependem da interação e cooperação entre governos, sociedade, academia e o setor empresarial. Além disso, os custos associados à proteção das

*O autor agradece a Flavia de Holanda Schmidt pelas valiosas contribuições e sugestões para o aperfeiçoamento deste trabalho.

[1] Técnico de Planejamento e Pesquisa da Diretoria de Estudos e Políticas Setoriais, de Inovação, Regulação e Infraestrutura (Diset) do Ipea.

[2] Pequenos dispositivos computacionais, ou sistemas embarcados, que buscam integrar a informática ao cotidiano das pessoas de forma muito natural para auxílio ou conforto ao ser humano.

redes e sistemas informacionais podem se tornar demasiadamente elevados para serem conduzidos apenas pelos setores não governamentais. Tem-se, assim, a necessidade de atuação do Estado na promoção de políticas de incentivo que conduzirão a sociedade e o próprio governo a um ambiente virtual mais seguro.

O governo brasileiro tem se mobilizado para fortalecer a proteção no espaço cibernético em território nacional. Em 2008, foi publicado o decreto 6.703, que aprovou a Estratégia Nacional de Defesa (END)[3] com o objetivo de elaborar um plano de defesa focado em ações estratégicas de médio e longo prazo para modernizar a estrutura nacional de defesa. Foram elegidos três setores estratégicos para defesa nacional: nuclear, espacial e o cibernético.

Conhecer os mecanismos utilizados para a realização de ataques cibernéticos é fundamental para a construção de sistemas de proteção robustos. Isso porque os sistemas de proteção são construídos a partir da eliminação de pontos de vulnerabilidade que podem ser utilizados por atacantes. Então, a rigor, ataque e defesa cibernética compõem dois lados de uma mesma moeda.

A seguir, na seção 2, é apresentado um resumo sobre o surgimento do setor cibernético e algumas considerações sobre proteção no ambiente virtual. Na seção 3 é apresentado o conceito de arma cibernética de ataque ou defesa e sua classificação em relação aos alvos. Em seguida, na seção 4, são apresentadas algumas habilidades necessárias para o desenvolvimento de arma cibernética de alvo específico, para ataque ou defesa. Por último, na seção 5, são apresentadas as considerações finais do texto.

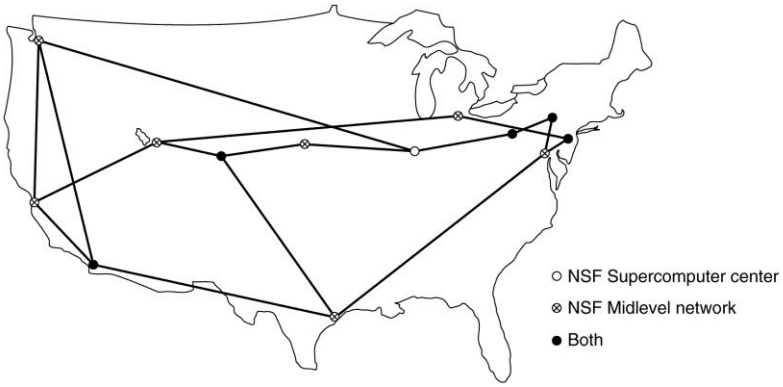
2. SEGURANÇA E DEFESA NO ESPAÇO CIBERNÉTICO

As primeiras redes de computadores tiveram início no final da década de 1950. No auge da Guerra Fria, o Departamento de Defesa dos Estados Unidos queria uma rede de controle e comando capaz de sobreviver a uma guerra nuclear. Nessa época, todas as comunicações militares passavam pela rede pública de telefonia, considerada vulnerável (Tanenbaum, 2011).

Em 1988 a NSFNET, a internet da época, conectava as redes locais dos grandes centros de pesquisa, universidades, museus e bibliotecas. Ou seja, há pouco mais de vinte anos praticamente ninguém sabia o que era internet, nem os usuários, nem seus idealizadores imaginavam que se expandiria tão rapidamente. Em 1988 internet apresentava a configuração mostrada na figura 1.

[3] Há uma nova versão da END em tramitação no Congresso: https://defesa.gov.br/index.php/ultimas-noticias/3869-24072012-defesa-politica-estrategia-e-livro-branco-de-defesa-nacional-conheca-os-documentos-enviados-pela-presidenta-da-republica-a-apreciacao-do-congresso-naciona.

Figura 1 - O *backbone* da NSFNET em 1988.



Fonte: (Tanenbaum, 2011)

O Brasil só experimentou a primeira transmissão de dados com o resto do mundo, pela internet, em 1991. Era uma conexão ponto a ponto, por cabo, voltada a troca de experiências entre a Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp) e o Fermilab[4], nos Estados Unidos. Em 1994, a internet finalmente transborda do mundo acadêmico e passa a ser comercializada em caráter experimental no país, a uma velocidade de 256 Kbps. Apenas em maio de 1995 o serviço começou a ser prestado de forma comercial pela Embratel (TecMundo, 2011). Percebe-se assim que a internet ainda está em uma fase muito inicial de desenvolvimento sendo, portanto, muito difícil prever os caminhos que irá seguir no futuro.

O Brasil está em um momento de grande transformação social e cultural. Conforme dados do Comitê Gestor de Internet no Brasil (CGI), em 2005, apenas 13% dos domicílios brasileiros tinham acesso à internet; já em 2011, foram registrados 38%. Em 2008, apenas 34% da população tinham acesso à internet, ao passo que em 2011 esse percentual sobe para 45%. Em 2008, apenas 1% da população tinha acesso à banda larga móvel (modem 3G); já em 2011, esse percentual sobe para 18% (CGI, 2012). Com isso, percebe-se que o Brasil somente começou a se inserir efetivamente no ambiente cibernético na última década.

A internet não foi inicialmente estruturada visando à proteção de dados e a segurança das informações de uma forma geral. Os protocolos atualmente utilizados (e. g., TCP/IP, UDP, RTP) são camadas de software que foram sendo inseridas como pequenas soluções para problemas locais (Tanenbaum, 2011). Isso se propagou tão rapidamente que hoje esse padrão é global. Como a infraestrutura que utiliza esse padrão é enorme, o custo de se recriar uma nova solução que atenda bem à realidade atual e futura torna-se quase impraticável.

Segurança e defesa no ambiente cibernético consistem em prever, identificar e eliminar possíveis vias de ataque a um sistema computacional (Conklin, 2006). Ou seja, reduzir ao máximo as vulnerabilidades existentes. Basicamente, a proteção contra ataques a alvos generalizados faz-se com medidas de proteção comuns, disponíveis no mercado, tais como antivírus, *antispyware, firewall, antispam*, etc. Já a proteção contra ataques a alvos específicos

[4] Laboratório de física especializado no estudo de partículas atômicas. Localiza-se em Illinois, nos Estados Unidos.

ou direcionados exige medidas singulares, ou seja, soluções dedicadas dependendo da infraestrutura que se objetiva proteger.

Paralelo à evolução da internet, observou-se ainda o rápido desenvolvimento dos dispositivos computacionais, chamados *hardwares*. A partir da década de 1980, os circuitos integrados ganharam força pela miniaturização de circuitos eletrônicos e queda de seus preços. Devido a essa rápida evolução, foi possível criar computadores e outros dispositivos pessoais e portáteis com valores bem mais acessíveis. Acredita-se que a computação quântica e a nanotecnologia sejam os caminhos para a evolução de novas gerações de dispositivos que hão de vir (Chen; Jonoska; Rozenberg, 2006).

Essa evolução do *hardware* ainda está proporcionando a massificação de dispositivos com alto poder computacional, além de capacidade para conexão com a internet. São *smartphones*, TV's, lavadoras, refrigeradores, automóveis, todos muito presentes no dia-a-dia das pessoas e, por vezes, já com alguma inteligência embarcada.

A essa integração sutil e natural entre os dispositivos que agregam as tecnologias de informações e comunicações ao cotidiano da sociedade dá-se o nome de ubiquidade (Sudha et al., 2007). Os sistemas ubíquos trazem a computação portátil ao cotidiano das pessoas, são também denominados computação pervasiva (*pervasive computing*), "tecnologia calma" (*calm technology*), "coisas que pensam" (*things that think*), "*everyware*" ou simplesmente inteligência ambiental.

Possivelmente, muito em breve, os computadores, como tradicionalmente conhecidos, cairão em desuso sendo substituídos por diversos dispositivos computacionais, espalhados por todos os ambientes, capazes de comunicar entre si pela internet (Costa, 2002).

A computação em nuvem ou *cloud computing* é um indicativo de que os novos aparelhos não necessitarão de uma unidade de memória local significativa. Isso porque todos os arquivos pessoais estarão sempre disponíveis remotamente, bastando contar com acesso à internet de alta velocidade para acessá-los em tempo real. Para que isso se torne realidade no cotidiano da maioria da população, é preciso garantir os requisitos básicos de defesa e segurança no ambiente virtual: confidencialidade, disponibilidade e integridade das informações.

Qualquer sistema computacional é suscetível a falhas (Mattos, 2008). Entretanto, o ser humano ainda é o elo mais frágil em toda a cadeia de fatores que compõem a proteção no ambiente cibernético (Miller, 2010). Por consequência, é também o mais explorado por *hackers*. Uma vez que os recursos são limitados, é preciso escolher adequadamente como investir de modo a maximizar a proteção.

De maneira geral, os custos envolvidos na proteção das informações dependem precipuamente do valor daquilo que se pretende proteger. Pelo prisma econômico, os recursos investidos na proteção de dados não podem ser superiores aos prejuízos financeiros e econômicos decorrentes de um eventual acesso indevido às informações vitais da entidade (governo, empresa, cidadão). Logo, caso a proteção se refira à Defesa Nacional de um país, os riscos decorrentes de perdas financeiras, insegurança pública, desordem social, instabilidade governamental, risco à soberania nacional, etc. devem servir como referenciais para balizar o montante a ser investido.

3. ARMAS CIBERNÉTICAS

Invasões cibernéticas são operacionalizadas por meio de software intencionalmente elaborado para a quebra de segurança de sistemas computacionais. É possível classificar esses *softwares* maliciosos, chamados *malwares*, pela quantidade de alvos (único/diversificados) e pelo potencial destrutivo (alto/baixo).

A contraparte, ou a defesa de sistemas, é feita também por meio da elaboração de *softwares*, mas desta feita, projetados para impedir que os *malwares* tenham êxito. Vale ressaltar que sistemas de proteção robustos só podem ser elaborados por quem entente os mecanismos e formas utilizados para ataque (Miller, 2010).

Assim como existem proteções a sistemas generalizados também existem os *softwares* de segurança e defesa específicos. Essa diferenciação implica diretamente na quantidade de recursos (pessoal, inteligência embarcada, tempo para desenvolvimento, dinheiro, etc.) empregados para se construir essa arma cibernética. Normalmente, quanto mais direcionada for uma arma (alvo específico a ser protegido ou atacado), mais cara ela se torna e ainda menores são as possibilidades de ela poder ser reutilizada sem modificações (Rid; McBurney, 2012).

A deterrência usual nestes casos faz lembrar aquela bastante comum no período da Guerra Fria: a simples crença de que a "nação inimiga" tem armas cibernéticas capazes de invadir, roubar informações sigilosas, interferir no funcionamento das infraestruturas críticas e, eventualmente, causar dano já pode ser suficiente para desestimular possíveis ataques exploratórios. Ou seja, o poder que uma arma de ataque cibernético tem também depende da percepção que a parte ameaçada tem sobre ela (Rid; McBurney, 2012).

Normalmente, os alvos de ataques cibernéticos evitam se expor para mitigar constrangimentos e não tornar públicas suas vulnerabilidades. Por outro lado a parte atacante também prefere manter-se anônima para evitar conflitos diplomáticos e exposição. Todavia, em geral, armas de ataque cibernético possuem potencial ofensivo menor do que comumente assumido (Miller, 2010).

Armas sofisticadas de ataque cibernético, assim entendidas como aquelas capazes de invadir e manipular sistemas fortemente protegidos, são extremamente complexas para serem desenvolvidas. Cada ambiente computacional possui suas próprias peculiaridades e singularidades. São inúmeras as possíveis combinações de *hardware* e *software* mesclando soluções modernas e arcaicas. A invasão, controle e manipulação de sistemas desse tipo exige um conhecimento profundo de todas as partes além de uma boa dose de sorte (Miller, 2010). Sorte, na medida em que os diversos tipos de "iscas" lançadas pelos atacantes precisam ser "mordidas" pelos alvos.

Assim, ataques direcionados são muito mais difíceis de serem implementados do que normalmente se imagina. Como resultado dessa complexidade, decorrem altos custos de desenvolvimento. Além disso, uma arma cibernética de aplicação específica precisa ser desenvolvida em absoluto sigilo, pois se a engenharia de ataque for descoberta, o processo de proteção normalmente é muito rápido. Todos os trabalhos de investigação, elaboração de software, inteligência embarcada, mecanismos de camuflagem, que podem custar milhares de

dólares e anos de desenvolvimento, normalmente são inutilizados em horas a partir da identificação das vulnerabilidades que estão sendo exploradas.

Assim, afirmações a respeito do baixo custo inerentes aos ataques cibernéticos devem ser consideradas com muito cuidado. Outro fator que corrobora isso é que, diferentemente das armas convencionais, as de ataque cibernético possuem uma vida útil muito curta. Elas praticamente perdem o seu valor a partir de sua identificação ou utilização.

Como exemplo de arma para alvos generalizados pode-se citar o ILOVEYOU. Em maio de 2000, um estudante filipino de 24 anos de idade desenvolveu sozinho esse vírus. O código rapidamente se espalhou por cerca de 45 milhões de plataformas utilizando o sistema operacional *Windows*. O "*love bug*", assim denominado pela imprensa, se propagou ao se passar por um *e-mail* de uma carta de amor advinda de uma fonte conhecida e, ao infectar o sistema, alterava arquivos de áudio e imagem com códigos maliciosos e assim se replicava (Rid e McBurney (2012)). O objetivo do vírus não era controlar ou dominar algum sistema, apenas causar danos generalizados.

Assim como o "*love bug*", a maioria dos vírus atualmente conhecidos são desenvolvidos para alvos generalizados. Por exemplo, os vírus de coleta de informações bancárias, tão difundidos no Brasil, são desenvolvidos para se espalharem indiscriminadamente e apresentam mecanismos mínimos ou inexistentes de camuflagem ou autoproteção. Isso faz com que os custos de desenvolvimento caiam significativamente. Ainda assim, muitas vezes, conseguem atingir seus objetivos, pois ainda há uma parcela significativa de internautas desprotegidos ou ingênuos.

Todavia, armas de ataque cibernético a alvos generalizados normalmente não conseguem invadir e manipular sistemas críticos. O que comumente é noticiado como invasão a sistemas de instituições relevantes no cenário mundial são, quase sempre, ataques direcionados. Notadamente, não é possível afirmar que armas cibernéticas de alvos generalizados sejam ineficazes contra as infraestruturas críticas. Todavia, caso consiga afetá-las, a princípio, caracteriza-se como um incidente, ou um efeito colateral.

Um exemplo típico de arma direcionada é o STUXNET. Este vírus foi projetado especificamente para atacar o sistema operacional SCADA[5], utilizado para controlar as centrífugas de enriquecimento de urânio iranianas. Há diferenças enormes entre vírus como o ILOVEYOU e o STUXNET. Este, ao contrário do primeiro, possuía um alvo específico, com estratégia de abordagem própria e mecanismos de interferência nos sistemas físicos, além de sistemas de autoproteção e camuflagem para que não fosse descoberto até atingir os objetivos. Apesar disso, não contava com mecanismos de aprendizagem, ou inteligência autônoma, nem auto-mutação, características esperadas nas próximas gerações de vírus. Este tipo de sofisticação faz com que os recursos necessários e os custos de produção dessas duas classes de vírus sejam absolutamente distintos.

Nesse sentido, uma das principais diferenças entre armas de alvos generalizados e específicos é a presença ou ausência de controle do processo. Assim, o que para uma é apenas um incidente para a outra pode ser a finalidade. Por isso, é necessário preparar-se e proteger-se de todos os tipos de ataques cibernéticos.

[5] Sistema de supervisão e aquisição de dados largamente utilizado em ambientes industriais.

O custo de defesa segue, em parte, a mesma lógica dos custos para ataque. A proteção contra um inimigo disposto a investir tempo e recursos para investigar as vulnerabilidades de seu alvo, comprar informações, minar lentamente a infraestrutura para então explorar as brechas encontradas, exige muito mais cuidado e recursos do que se proteger de exploradores de vulnerabilidades genéricas.

Portanto, conhecer os mecanismos de ataque torna-se fundamental para a construção de sistemas de proteção robustos. De fato, ataque e defesa compõem dois lados de uma mesma moeda. A seguir, são apresentados alguns recursos básicos para a produção de uma arma de defesa ou ataque cibernético.

4. HABILIDADES NECESSÁRIAS PARA DEFESA OU ATAQUE CIBERNÉTICO

Como já explicado, a singularidade de uma arma cibernética e sua engenharia de ataque ou defesa são seus aspectos mais valiosos. Assim, é evidente que encontrar documentos oficiais de acesso público com relatos de requisitos e procedimentos para se elaborar uma arma cibernética é algo, no mínimo, improvável.

Dessa forma, a descrição feita nesta seção baseia-se especialmente em um estudo apresentado por Charlie Miller (2010), pesquisador independente, apresentado na *Conference for Cyber Conflict 2010*. Nesse estudo, o autor descreve um planejamento de capacitações humanas para se desenvolver uma arma de ataque cibernético. É oportuno relembrar que o objetivo principal deste trabalho não é incentivar a capacitação ofensiva brasileira e sim fazer um paralelo entre as habilidades utilizadas em mecanismos de ataque, que por sua vez deverão ser combatidos na formação de equipes para a defesa cibernética.

Conforme Miller (2010), ataques a redes de alta segurança exigem muita pesquisa e planejamento. E isso não se faz da noite para o dia. Diversas ferramentas de espionagem (troca de informações, varreduras, etc.) são facilmente identificadas se estiverem em plena operação, mas podem passar despercebidas se operarem lentamente. Outra estratégia normalmente utilizada por atacantes é se passar por *hackers* medianos ou ingênuos para explorarem o ambiente, especialmente nas fases iniciais de desenvolvimento. Assim, mesmo se forem descobertos explorando vulnerabilidades, os custos são baixos e é mais difícil uma ação isolada ser interpretada como uma manobra governamental, militar ou algo mais sofisticado. Assim, para equipes de defesa, qualquer atividade suspeita precisa ser investigada com atenção.

É preciso conhecer, em profundidade, o sistema a ser atacado ou defendido. Por exemplo, se o objeto da ação são bancos, é preciso conhecer bem os sistemas financeiros. Se o objeto for um sistema industrial, é preciso conhecer o sistema SCADA ou algum outro que seja utilizado, e assim por diante; descobrir quais os princípios, requisitos e definições inicialmente adotadas pelos fabricantes de *softwares* ao serem construído; identificar qual o *hardware* e *software* que os principais roteadores de internet utilizam; definir qual sistema defensivo e de monitoramento utilizados. O mapeamento dessas questões ajudará a montar um panorama de quão difícil, quais as possíveis vulnerabilidades e quais os recursos necessários para criar uma arma cibernética com razoáveis possibilidades de êxito. Seja para ataque ou para defesa.

Mesmo os sistemas mais seguros, especialmente aqueles isolados fisicamente da internet, ainda podem ser explorados e atacados. O vírus pode ser introduzido por meio de dispositivos móveis de armazenamento de dados como *flash drive*, por exemplo. Tentativas de conectar o sistema à internet também podem ter sucesso por meio de dispositivos móveis como *smartphones* utilizando rede 3G, 4G ou mesmo satélites.

Assim, diversas são as possibilidades tecnicamente possíveis de se infiltrar e dominar uma rede. Sejam redes mais ou menos seguras, todas são susceptíveis a falhas frente a um atacante bem capacitado, preparado e motivado a invadir.

A seguir são listadas algumas habilidades envolvidas no processo de elaboração de uma arma cibernética.

a. Analistas de vulnerabilidades: são profissionais dedicados a encontrar falhas no sistema alvo. Esses especialistas são profissionais que fazem varredura utilizando análise *fuzzy*[6] ou analítica atrás de qualquer tipo de falha de sistema. Pessoas com esse talento são difíceis de ser encontradas ou mesmo formadas. Assim, a atuação em parceria formando redes de colaboração entre governo, academia e setor privado é extremamente necessária no momento de seleção ou identificação de talentos.
b. Desenvolvedores de *exploits*[7]*:* elaboram ferramentas para explorarem as vulnerabilidades encontradas. Essa equipe dedica-se a tornar as vulnerabilidades identificadas em pontos de exploração altamente confiáveis. Determinam como e quando explorar as falhas encontradas e as jamais exploradas (*0-day*). Possuem habilidade para construírem exploradores em várias plataformas (Windows, Mac OS, Linux, Unix). Novamente, esta? equipe precisa ser altamente capacitada, habilidosa e discreta, de modo a avançar nos mecanismos de exploração sem desperdiçar as vantagens até então adquiridas e recursos empregados. Mesmo que para a proteção de um sistema não haja a necessidade de se desenvolver *exploits*, ainda assim é desejável manter na equipe alguém com conhecimento na área.
c. Coletores de *bots (ataque):* "escravizam" servidores alheios de modo a dispor de alto poder computacional nos momentos críticos de ataque. A utilização de servidores espalhados pelo mundo é uma estratégia para confundir os profissionais de proteção e esconder os atacantes. Eles utilizam os exploradores desenvolvidos anteriormente no lado dos clientes (parte atacada) para dominar a maior quantidade de computadores e dispositivos possível, tornando-os escravos, também chamados de zumbis ou, simplesmente, *bots*. A entrega dos *exploits* é, normalmente, feita via *spam* por correio eletrônico, *banners* de propaganda comprometidos ou pela invasão do sistema e implantação direta do *malware*. Por exemplo, a medida adotada pelos desenvolvedores do STUXNET foi espalhar o vírus por todos os computadores do Irã, e região, para que, ocasionalmente, ele fosse conduzido por algum funcionário em um *flash drive* comprometido até à usina nuclear do país, uma vez que ela era isolada fisicamente da internet ("isca", explicado na seção 3).
d. Mantenedores das redes de *bots (ataque):* fazem com que as redes já capturadas não sejam perdidas para outros grupos ou saneadas por meio dos sistemas de proteção e defesa. O conjunto de máquinas e dispositivos *bots* estará em constante mudança e transformação por meio de novos dispositivos, aplicativos, atualização de sistemas, etc. Esse grupo é responsável por monitorar o tamanho e a qualidade das redes de *bots* bem

[6] Tipo de análise em que se utiliza lógica multivalorada e envolve conceitos estatísticos principalmente na área de Inferência.
[7] Programas desenvolvidos para explorar as vulnerabilidades encontradas.

como a densidade geográfica dentro e fora do país ou região. Tentam manter esses sistemas sempre disponíveis e, quando necessário, até eliminar outros *malwares* e vírus em operação. Ou seja, fazem o "saneamento" do sistema para eles sejam os únicos exploradores.

e. Operadores de rede: esse pode ser considerado o grupo de elite dos invasores (*pentesters*). Normalmente, utilizam ferramentas customizadas para invasões de alto nível e ainda vulnerabilidades inéditas ou jamais exploradas (*0-day*). Essa equipe precisa ter o conhecimento e a compreensão de todo o funcionamento da rede ou sistema. Também tem a função de expandir as áreas já invadidas utilizando ferramentas ativas e passivas de escaneamento e penetração de rede.
f. Equipe de apoio remoto: responsável por configurar e orquestrar ações espalhadas pelo mundo para que o comando de operações não fique centralizado. Isso dificulta ainda mais a identificação de responsáveis e autores, caso parte da ação seja identificada.
g. Equipe de desenvolvedores: utilizaram os *bots* fazendo uso de uma variedade de meios e modos de comunicação. Os desenvolvedores elaboram ferramentas customizadas para serem utilizadas por pessoas menos capacitadas. Essa diversificação serve para camuflar a ação global, caso algumas das ações isoladas sejam identificadas. Essa diversidade de equipes, muitas vezes sem comunicação entre si, é intencional para se conseguir uma diversidade de soluções para o mesmo objetivo. Além disso, a modularização de etapas e ferramentas possibilita a contribuição de diversos atores sem que eles mesmos saibam o objetivo final do projeto.
h. Equipe de testes: montada a plataforma básica de ataque, parte-se para a verificação da efetividade dos componentes implantados e validação da plataforma criada. Para isso, uma equipe de testes, necessariamente distinta dos desenvolvedores, entra em ação. Os testes de funcionalidade e confiabilidade são feitos nos exploradores desenvolvidos, redes de *bots* adquiridas e *RATs* (*remote access trojan*) instalados. Testam as ferramentas utilizadas frente à maior variedade de antivírus, sistemas de proteção e atualizações de *software* para garantir a discrição e camuflagem do ataque, pelo menos até que os objetivos sejam atingidos.
i. Consultores técnicos: muitas vezes consultores são necessários para repassarem informações confidenciais ou mesmo específicas de determinado sistema. São especialistas em hardware e software de sistemas específicos, atuais ou obsoletos, que podem ser explorados. São exemplos, profissionais que conhecem o funcionamento de sistemas como: SCADA, gestão de saneamento, defesa civil, telefonia, médico-hospitalares, aviônicos, geração, transmissão e distribuição de energia, etc. Não precisam integrar a equipe de modo contínuo, são chamados apenas para "vender informações".
j. Administradores de sistemas: mantêm os sistemas em operação e atualizados. Quando no lado ofensivo, instalam softwares nos clientes e alvos. Gerenciam os testes de redes e sistemas.

5. CONSIDERAÇÕES FINAIS

Este texto teve por objetivo apresentar os riscos e ameaças inerentes às tecnologias da informação e comunicação e ainda buscou mostrar como essas ameaças podem ser mitigadas ao se conhecer os mecanismos normalmente utilizados em ataques cibernéticos.

Fatos mostram que o ambiente cibernético tem se tornado, a cada dia, o maior portador de

conflitos internacionais. O Brasil, não somente pelas necessidades internas, mas também por sua relevância internacional, não pode prescindir de políticas consistentes voltadas para esta questão.

A dependência da sociedade e do governo pelas tecnologias da informação e comunicação é determinante da responsabilidade do Estado pela segurança cibernética em território nacional. Na medida em que o bem estar e a segurança da sociedade passam a depender da segurança cibernética, a questão torna-se um dever do Estado.

Atualmente, praticamente todas as infraestruturas críticas que dão suporte ao progresso, à paz e à segurança da sociedade dependem dos sistemas computacionais. Ademais, a tendência é que essa dependência cresça ainda mais com o passar dos anos.

Independente de como a tecnologia será no futuro, as componentes da segurança da informação – confidencialidade, disponibilidade e integridade – deverão ser garantidas. Isso é fundamental para que a sociedade possa usufruir das facilidades e benefícios dos sistemas informatizados.

Criar sistemas de segurança robustos exige não apenas conhecimento, mas também o domínio de táticas e estratégias sofisticadas de ataque. Isso porque os mecanismos de proteção são construídos a partir da identificação das falhas e vulnerabilidades no próprio sistema e as formas que elas poderiam ser exploradas em um ataque. Ou seja, a melhor forma de estar capacitado para se defender é conhecer os mais variados meios, instrumentos e mecanismos de ataque.

São várias as habilidades exigidas de uma equipe dedicada à proteção de um sistema computacional, especialmente de infraestruturas críticas. Sabe-se ainda que profissionais com tais habilidades são difíceis de serem recrutados ou mesmo formados. Assim, a atuação em parceria formando redes de colaboração entre governo, academia e setor privado é extremamente necessária no momento de seleção ou identificação de talentos.

Quando se trata de segurança e defesa cibernética a capacitação humana vale mais do que investimento em equipamentos e/ou sistemas de proteção. Além disso, estudos mostram que investir na capacitação do fator humano constitui medida mais eficaz e econômica do que aplicar o recurso puramente em equipamentos (Takemura; Osajima; Kawano, 2008). Isso porque o fator humano continua sendo o elo mais frágil de qualquer sistema de proteção.

As normas e padrões estabelecidos pela ISO 27000[8] são um bom referencial para operadores e mantenedores de sistemas computacionais. O constante treinamento e aperfeiçoamento de profissionais é medida indispensável para a segurança ou defesa de qualquer sistema.

Como explicado, qualquer sistema computacional é susceptível a invasões. Com dedicação, paciência e habilidade qualquer sistema pode ser invadido. Por outro lado, a grande maioria dos ataques identificados é feita por amadores que utilizam ferramentas prontas, disponíveis na internet (Hoepers, 2011). Assim, apesar de não garantir a absoluta segurança, bons sistemas de

[8] A Norma ISO 27000 é um padrão internacional sobre as boas práticas na Gestão da Segurança da Informação, que levam empresas ao nível máximo de excelência internacional em Segurança da Informação.

proteção são capazes de resistir à grande maioria das tentativas de invasões diariamente realizadas nos mais diversos sistemas.

No caso brasileiro, nas mais de 320 redes do Governo Federal são identificados em torno de três mil incidentes relevantes de segurança por mês (GSI/PR, 2013). Além disso, é possível que existam inúmeros ataques não identificados.

A proteção contra armas cibernéticas de alvos generalizados pode ser feita por meio da instalação e, principalmente, a manutenção de sistemas de proteção prontos no mercado, como *antivírus*, *antispyware*, *firewall*, anti-rootkit, *antispam*, etc. Entretanto a proteção contra ataques específicos ou inimigos persistentes exige medidas singulares, e, nesse caso, o investimento deve ser proporcional aos valores (social, financeiro, econômico, moral, etc.) daquilo que se objetiva proteger.

Demandas governamentais perenes de sistemas de segurança e defesa cibernética poderão auxiliar a estruturação e o fortalecimento da indústria nacional de segurança e defesa cibernética. Soluções de proteção visando especialmente infraestruturas críticas deveriam conter proporções razoáveis de tecnologias desenvolvidas nacionalmente, de modo a eliminar, gradativamente, a dependência internacional.

Esse nível de proteção necessária contra possíveis inimigos habilidosos e persistentes, apesar de constituir a minoria dos ataques identificados, exige maior atenção governamental, especialmente quando se trata de infraestruturas críticas. Isso porque o desenvolvimento de armas de defesa cibernética para tais sistemas implica no autoconhecimento das fraquezas, incluindo aquelas que nem mesmo sabemos que possuímos.

BIBLIOGRAFIA

AMORIM, C. **ASPECTOS DA DEFESA CIBERNÉTICA**, 24 out. 2012. Disponível em: <https://www.defesa.gov.br/arquivos/2012/Pronunciamentos/Ministro_defesa/outubro/discurso_aspectos_defesa_cibernetica_24_outubro_2012.pdf>. Acesso em: 26 out. 2012

CGI. **Pesquisa sobre o uso das tecnologias de informação e comunicação no Brasil : TIC Domicílios e TIC Empresas 2011**. São Paulo: Comitê Gestor da Internet no Brasil, 2012.

CHEN, J.; JONOSKA, N.; ROZENBERG, G. **Nanotechnology: Science and Computation**. [S.l.] Springer, 2006.

CONKLIN, A. **Cyber defense competitions and information security education: An active learning solution for a capstone course**System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on. **Anais**...2006Disponível em: <http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1579743>. Acesso em: 10 maio. 2013

COSTA, A. M. N. DA. Revoluções tecnológicas e transformações subjetivas. **Psicologia: teoria e pesquisa**, v. 18, n. 2, p. 193–202, 2002.

GSI/PR. **ESTATÍSTICAS DE INCIDENTES DE REDE NA APF – 4° TRIMESTRE/2012**. Brasil: CTIR/DSIC/GSI/PR, 2013. Disponível em: <http://www.ctir.gov.br/estatisticas.html>.

HOEPERS, C. **Segurança da Internet no Brasil**IPEA, 9 ago. 2011. Disponível em: <http://www.cert.br/docs/palestras/certbr-ipea2011.pdf>. Acesso em: 29 ago. 2011

MATTOS, D. M. F. Virtualização: VMWare e Xen. **Grupo de Teleinformática e Automação da UFRJ**, p. 13, 2008.

MILLER, C. **How to build a cyber army to attack the U.S.**Conference for Cyber Conflict, , 2010. Disponível em: <https://www.defcon.org/images/defcon-18/dc-18-presentations/Miller/DEFCON-18-Miller-Cyberwar.pdf>. Acesso em: 21 maio. 2012

RID, T.; MCBURNEY, P. Cyber-Weapons. **The RUSI Journal**, v. 157, n. 1, p. 6–13, 2012.

SUDHA, R. *et al.* **Ubiquitous Semantic Space: A context-aware and coordination middleware for Ubiquitous Computing**Communication Systems Software and Middleware, 2007. COMSWARE 2007. 2nd International Conference on. **Anais**...jan. 2007

TAKEMURA, T.; OSAJIMA, M.; KAWANO, M. Empirical Analysis on Information Security Countermeasures of Japanese Internet Service Providers. Discussion Paper. p. 18, nov. 2008.

TANENBAUM, A. S. **Computer networks**. 5. ed. [S.l.] Prentice Hall PTR, 2011.

TECMUNDO. **20 anos de internet no Brasil: aonde chegamos?** Disponível em: <http://www.tecmundo.com.br/internet/8949-20-anos-de-internet-no-brasil-aonde-chegamos-.htm>. Acesso em: 31 jan. 2013.